

UNITED STATES DISTRICT COURT

FILED

for the
Western District of Texas

2015 DEC 14 PM 1:28

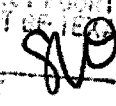
In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

414A W. Dittmar Road, Austin, Texas 78745,
and all buildings, structures, vehicles, and
appurtenances on the curtilage thereof

Case No.

1:15-M-627

CLERK OF DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY 

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
414A W. Dittmar Road, Austin, Texas 78745, and all buildings, structures, vehicles, and appurtenances on the curtilage thereof, which is more specifically described in Attachment A.

located in the Western District of Texas, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2252A

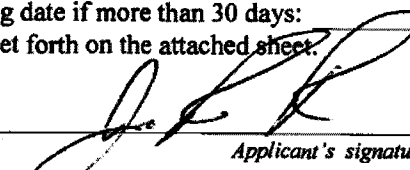
Offense Description
Possession/Receipt/Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

JAMES ROSS BEHRENS, Task Force Officer, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12-14-2015

City and state: Austin, Texas


Judge's signature
Mark Lane
United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

SEALED

In the Matter of the Search of:

The premises located at
414A W. Dittmar Road,
Austin, Texas 78745,
and all buildings, structures, vehicles, and
appurtenances on the curtilage thereof

§
§
§
§
§
§
§

NO. 1:15-M-627

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, James Ross Behrens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of a search warrant for the premises located at 414A W. Dittmar Road, Austin, Texas 78745, and all buildings, structures, vehicles, and appurtenances on the curtilage thereof (hereinafter the "Subject Premises"), which is more specifically described in Attachment A, and is located in the Western District of Texas. As set forth herein, there is probable cause to believe that at the Subject Premises there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) (receipt and distribution of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography); and 2252A(a)(5)(B) and (b)(2) (possession of, knowingly access, conspiracy to access, or attempted access with intent to view child pornography), as set forth in Attachment B hereto.

2. I have been certified and licensed as a Texas Peace Officer since 1996. Your Affiant is currently employed with the Texas Attorney General's Office Child Exploitation Unit

where he conducts investigations primarily involving crimes against children such as sexual exploitation of children and child pornography. Also at this time, I am assigned as a Task Force Officer to the Federal Bureau of Investigation Violent Crime Child Exploitation Task Force located at the Austin Resident Agency of the San Antonio Division, Texas. By being on the Task Force, I carry a commission as a Special Deputy United States Marshal of the United States Department of Justice and am charged with the duty of investigating violations of the laws of the United States as stated in Title 28, Federal Code of Regulations. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, §§§ 2251, 2252, and 2252A. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have participated in the execution of numerous search warrants for documents and other evidence, including computers and electronic media, in cases involving child pornography and the sexual exploitation of children. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. At all times in this affidavit the phrase "child pornography" is used solely as shorthand for visual depictions of actual minors engaged in sexually explicit conduct, as these terms are defined in Title 18, United States Code, Section 2256.

4. The statements contained in this affidavit are based in part on information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/analysts and

computer forensic professionals; and my experience, training and background as a law enforcement officer. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation, but only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of one or more violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), and 2252A(a)(5)(B) and (b)(2) are presently located at the Subject Premises.

5. Based on the facts presented below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A relating to the receipt, possession, distribution, transportation of child pornography, knowingly access or attempted access with intent to view child pornography, and conspiracy to commit said offenses, exists within the Subject Premises. I request authority to search the entirety of the Subject Premises, including any residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

6. The instant investigation, described more fully below, involves an Internet-based website referred to as "Website A".¹ The instant investigation has revealed that a user of the Internet account at the Subject Premises has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network.

¹ The actual name of "Website A" is known to law enforcement. Investigation into the users of this website and other websites remains ongoing and disclosure of the names of the sites would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. §§ 2252A, relating to material constituting or containing child pornography.

a. 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

b. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

8. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post

messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

f. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (“DNS”) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (“IP”) address so the computer hosting the web site may be located, and the DNS server provides this function.

g. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes

programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

p. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

q. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

s. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

u. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

x. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

COMPUTERS AND CHILD PORNOGRAPHY

9. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

10. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

11. With digital cameras, images of child pornography can be transferred directly onto a computer. Images and videos produced with "analog" photographic equipment (e.g., using film, videotape, DVD, or other analog image-capturing product) can quickly and easily be converted into a digital format and stored as electronic data on a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made with literally millions of computers around the world.

12. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Other storage media, including, but not limited to, CDs, DVDs, flash storage devices (commonly called "thumb drives"), memory cards, and portable external hard drives, are also used to copy, store, transport, and transmit digital images.

13. The Internet affords individuals several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

14. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's

computer in most cases.

15. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the

files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

16. I know that data files, including digitized images, correspondence, records, communications, and other matters sought by this Warrant, can be stored in a variety of digital formats on a computer using various software applications. For example, digital still images are commonly created and stored as JPEG files, and identified by .jpg or .jpeg in the filename suffix. Digital still images may also be created, converted, or stored, among other things, as an Adobe Acrobat file (using the suffix .pdf); embedded within a word processing document (using the suffix .wpd, .doc or .docx); or converted to another graphics file format (.gif or .tif). In addition, data filenames typically include a suffix associated with the application that created or modified the file (e.g., XXXX.pdf indicates a file associated with Adobe Acrobat). A filename, however, can be manipulated to include a suffix that conceals its true format, or is not readily recognized by or associated with any software application. Accordingly, because digitized versions of items sought by this Warrant can be created and/or stored in any number of digital file formats, it is necessary to search every data file stored on a computer or other data storage device to locate and seize such items.

17. Mobile communication devices are commonly used for both personal and business use. These devices range from simple mobile telephones to complex devices encompassing numerous technologies in one hand-held device. They are electronically powered and typically combine the ability to store and transfer data along with serving as a communications facility. Mobile communication devices are essentially ultra small computers,

as proven by the following facts:

a. Mobile communication devices use micro processors similar to computers. These processors are produced by the same companies that produce them for computers, like Intel, for example. The user interfaces with the device using a keyboard, much like a typical laptop or desktop computer and uses a directional pointer, much like a computer mouse.

b. The various technologies that can be incorporated into these devices include: telephones, still cameras, video cameras, Internet access (including e-mail, web surfing, file transferring), wireless data transfer between devices (such as Bluetooth technology, cellular transmission and infrared), data storage (including text files, image files, video files, spreadsheets, databases), data organizers (address, telephone, calendar), messaging, audio recorders, and music players (such as MP3 players). The picture quality of images viewed on these devices can be quite excellent, as technology allows high resolution, color images, both still and video, to be viewed.

c. Mobile communication devices require the user to subscribe to services from a service provider. Such services can include telephone service (and all associated services such as voice mail, call waiting, caller ID, call forwarding, contact or address book), e-mail, Internet access, text messaging, data transfer (including the ability to transmit digital images and videos), and other fee-based services.

d. Mobile communication devices can communicate with other devices such as computers, telephones, personal digital assistants (PDAs), electronic peripherals such as printers, other mobile communication devices, and other such electronic or digital based devices. The methods typically used to connect with other devices include radio signals, Bluetooth wireless technology, and infrared (IR) signals.

e. Mobile communication devices generally use one of two popular operating systems, Android and Apple iOS. These operating systems allow the device to operate properly and to communicate with other devices. Both Android and Apple iOS have a component which is loaded onto a computer. This allows the user to enter or change data using the computer or the device, then transfer this data easily to/from the computer and the device. The procedure is called synchronization. The devices are typically sold with a cable which allows the user to synchronize the data on the device with their computer. These devices can also connect with a computer via infrared or network Internet Protocol (IP), allowing the user to synchronize with the host computer from anywhere a cellular connection is made.

f. Mobile communication devices also have what is called "volatile memory" similar to computers. Volatile memory allows data to be stored while the device is powered on, then removes the data once the device is turned off. Not all data is stored in volatile memory, however, data can also be stored (and typically is stored) on memory cards. Mobile communication devices use memory cards just as a computer uses a hard drive. Once a memory card is inserted into the device, the user may store data on that card indefinitely, up to the storage capacity of that card. These cards can store up to 128 gigabytes of data – or more. A card of this size could theoretically hold thousands of high resolution image and video files. The card may be removed and kept to use later, while another card may be inserted into the device. In this way, a user can have numerous cards storing volumes of data, any of which he can insert into a device when he wishes to access that data.

g. These devices are readily available to the public and are priced in a wide range allowing individuals from all economic levels to obtain the devices and the services associated with the devices.

h. Based on my training and experience involving mobile communication devices, I know these devices are commonly transported by the user on their person, in the user's vehicle, and are connected to the user's computer or computers via a USB connection cable. Users typically maintain software to communicate with the mobile communication devices on the residence and work computers and then transfer or synchronize the data on the device with the data on the computers. The purpose of this procedure is so the user has all data on the device and any and all computers at the user's disposal. This data can include personal or business contacts, calendar entries, notes or memos, and images. Users typically transport the device between their residence and business on a daily basis. As this device serves as a mobile telephone, users typically carry the device on their person and maintain it nearby when at work or home. It is the practice of many users to connect the device to the synchronization cable attached to their computer(s) while at home or work, for the most efficient transfer of data and updating of their files. I have has been involved in cases where mobile communication devices have contained images downloaded from a personal computer.

18. Based on my training and experience, I know that cellular telephones can be used to transmit written messages ("texting") as well as images and/or videos. Cellular telephones have the capacity to store voice mail messages, names, telephone numbers, addresses, sent and received text messages, and images on their internal memory. Many cellular telephones have the capability to capture digital photographic images and videos, store them in internal memory, and transmit them to one or more different cellular telephones. Some cellular telephones contain small removable memory cards that can be used to store data and images. I also know that individuals sometimes use cellular telephone to produce, send, and receive pornographic images of themselves and others.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS
WITH INTENT TO VIEW AND/OR PRODUCE, RECEIVE, DISTRIBUTE, OR
POSSESS CHILD PORNOGRAPHY**

19. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically

retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who distribute, transport, receive, possess child pornography, and access with intent to view, or who attempt to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

20. Based on the following, I believe that a user of the Internet account at the Subject Premises likely displays characteristics common to individuals who access with intent to view and/or possess, receive, or distribute child pornography. For example, the target of investigation:

- a. Became a user of "Website A", whose primary purpose was to advertise and distribute child pornography;

- b. Accessed "Website A" message threads containing child pornography and/or child exploitation material and a posting on this website.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Searches and seizures of evidence from computers commonly require agents/officers to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, thumb drives, portable hard drives, memory cards, diskettes, tapes, laser disks, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an

operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

22. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

23. Furthermore, because there is probable cause to believe that the computer(s) and its/their storage devices are all instrumentalities of crimes, they should all be seized as such.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

24. A user of the Internet account at the Subject Premises has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A.". There is probable cause to believe that a user of the Internet account at the Subject Premises knowingly access with intent to view child pornography on "Website A."

The Network²

25. "Website A" operated on a network ("the Network") available to Internet users

² The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

26. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its

³ Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

27. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user.

28. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Description of "Website A" and its Content

29. "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting

"Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

30. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

31. Upon accessing the "register an account" hyperlink, there was a message that

informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

32. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

33. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and "scat" refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

34. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The "last post" section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

35. A review of the various topics within the "[Website A] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

36. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

a. On February 3, 2015, a user posted a topic entitled "Buratino-06" in the forum "Pre-teen - Videos - Girls HC" that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

b. On January 30, 2015, a user posted a topic entitled "Sammy" in the forum "Pre-teen - Photos - Girls" that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis

of a male; and

c. On September 16, 2014, a user posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

37. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, "Website A" contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

38. "Website A" also included a feature referred to as "[Website A] Image Hosting." This feature of "Website A" allowed users of "Website A" to upload links to images of child pornography that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

39. Text sections of "Website A" provided forums for discussion of methods and

tactics to use to perpetrate child sexual abuse. For example, on January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

Court Authorized Use of Network Investigative Technique

40. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

41. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."

42. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

"marleyboy" ON "Website A"

43. According to data obtained from logs on "Website A," monitoring by law enforcement and the deployment of a NIT, a user with the user name "marleyboy" engaged in the following activity on "Website A."

44. The profile page of user "marleyboy" indicated this user originally registered an

account on "Website A" on February 23, 2015. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user "marleyboy" profile, this user was a Newbie⁵ Member of "Website A." Further, according to the Statistics section of this user's profile, the user "marleyboy" had been actively logged into the website for a total of approximately 14 hours 5 minutes between the dates of February 23, 2015, and March 04, 2015.

IP Address and Identification of User "marleyboy" on "Website A"

45. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on March 02, 2015 at 05:58 UTC, the user "marleyboy" engaged in the following activity on "Website A" from IP address 173.174.40.45, utilizing MAC Address: 74E50BC8D86C, Host Name: "Computer," Log-On ID: "Owner." During the session described below, this user browsed "Website A" after logging into "Website A" with a username and a password.

46. On March 02, 2015, the user "marleyboy" with IP address 173.174.40.45 accessed the post titled, "13 Year Old Paraguayan Strips Bare." Among other things, this post contained a link to a video purported to be of a juvenile girl removing her clothing.

47. During the following additional sessions, the user "marleyboy" also browsed "Website A" after logging into "Website A" with a username and password. During these sessions, the user's IP address information was not collected.

48. On March 4, 2015, the user "marleyboy" accessed the post "Valya thread." with the Thread ID 1514 which contained a link to an image that depicted an adult male inserting his

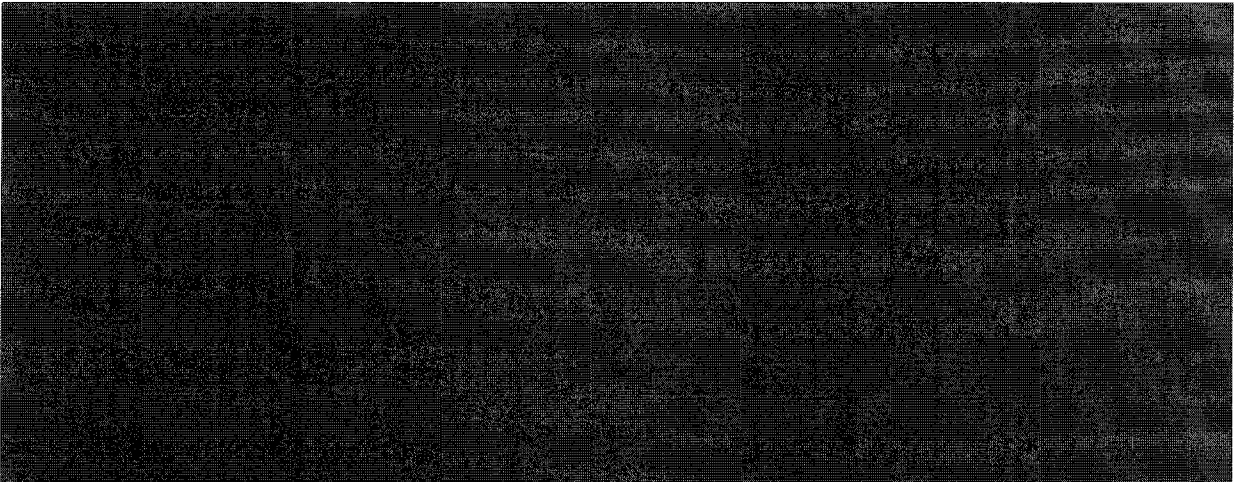
⁵ The title of a member was assigned based upon the total number of posts made by the particular member.

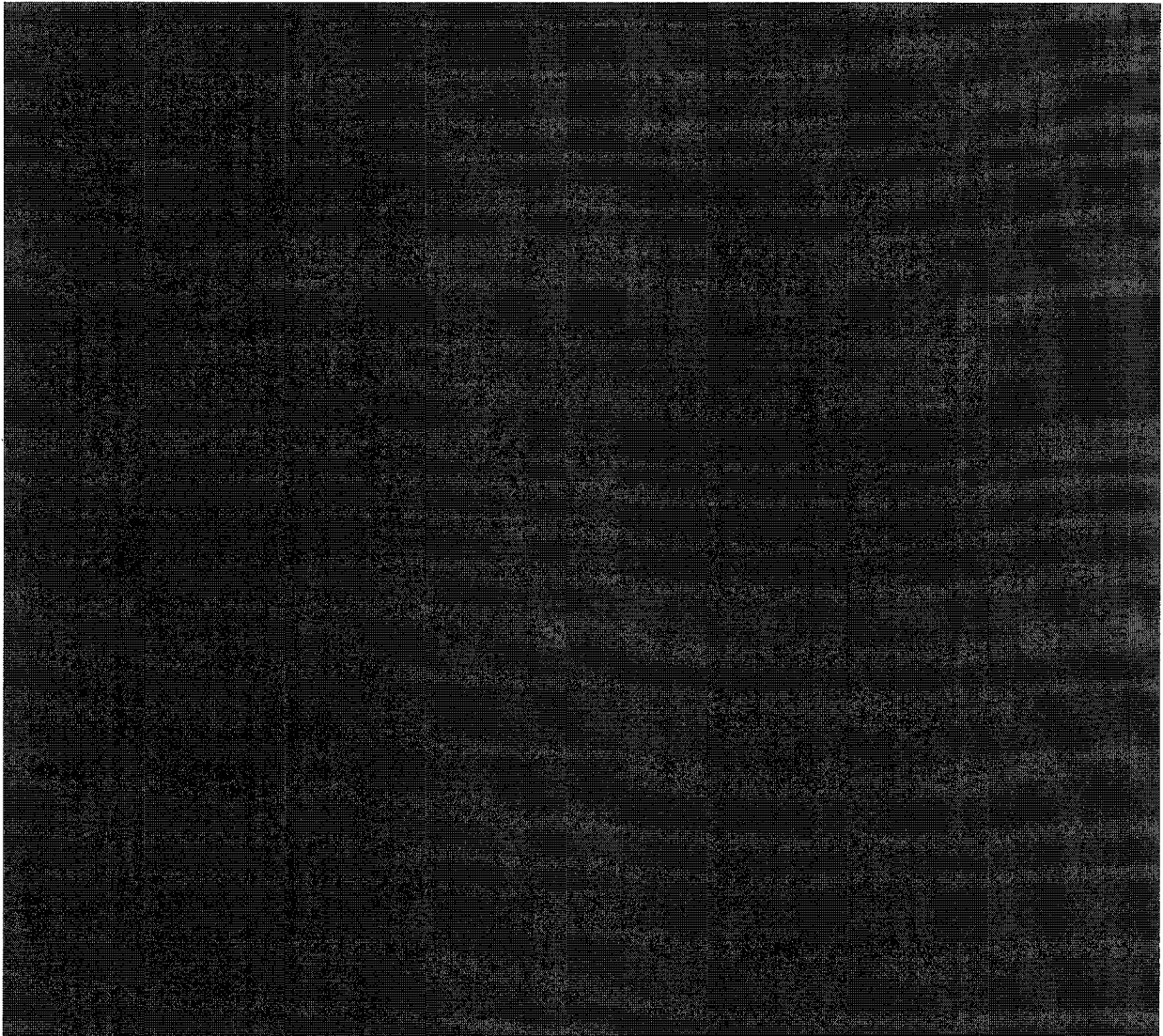
penis into the anus of a prepubescent girl depicted the minor engaging in genital-genital sexual intercourse and constituted child pornography.

49. On March 03, 2015, the user "marleyboy" accessed a post "[OFFER] Taking 'Girles [sic] cams' requests" with Thread ID 18375, containing a link to an image that depicted a phallic object being inserted into the vagina of a prepubescent girl, which depicted the minor engaging in genital-genital sexual intercourse and constituted child pornography.

50. Using publicly available websites, FBI Special Agents were able to determine that IP address 173.174.40.45 was assigned to Time Warner Cable, an Internet service provider ("ISP").

51. In March 2015, an administrative subpoena/summons was served to Time Warner Cable requesting information related to the subscriber to IP address 173.174.40.45 on March 2, 2015 at 05:58 UTC. According to the information received from Time Warner Cable the subscriber to the above IP address during the relevant time period was [REDACTED] at the Subject Premises. In October 2015, in response to another administrative subpoena/summons, Time Warner Cable confirmed that internet service was still being provided to the Subject Premises and the subscriber was [REDACTED]





CONCLUSION

55. Based on the aforementioned facts, there is probable cause to believe that one or more violations of 18 U.S.C. § 2252A have been committed and that evidence, fruits, and instrumentalities of said offenses, and contraband, namely, child pornography, may be found at the Subject Premises, which evidence is more specifically set forth in Attachment B to this affidavit.


56. Accordingly, I respectfully request that a search warrant be issued for the Subject

Premises, more particularly set forth in Attachment A, authorizing the search and seizure of the items listed in Attachment B.

57. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto may jeopardize the ongoing criminal investigation. Accordingly, I request that the Court issue an order that the search warrants, this affidavit, the application for search warrants, and all attachments thereto be filed under seal until further order of this court.

FURTHER AFFIANT SAYETH NAUGHT.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



JAMES ROSS BEHRENS
Task Force Officer
Federal Bureau of Investigation
Austin, Texas

Subscribed and sworn to before me at Austin, Texas, on this 14TH day of
December, 2015.



UNITED STATES MAGISTRATE JUDGE

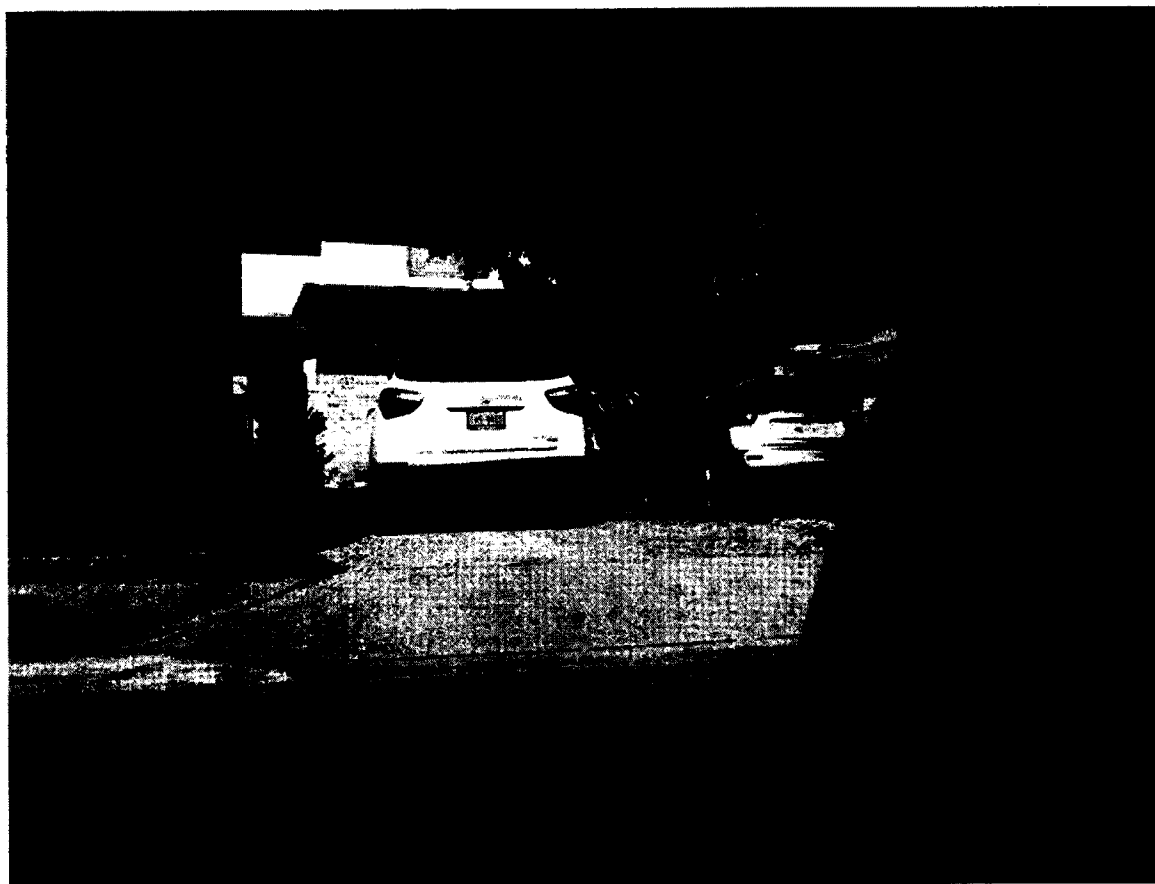
Mark Lane
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The premises known as at 414A W. Dittmar Road, Austin, Texas 78745, also referred to as Unit A of 414 W. Dittmar Road, is more particularly described as two-family, two-story duplex comprised of tan and brown brick on the lower level with tan hardie-siding on the upper level. The duplex faces south and has a driveway leading from the street (West Dittmar Road) to the two garage doors located in the middle. The front doors are located on the far left (west) and far right (east) of the duplex with a sidewalk leading up to each door from the driveway. Unit "A" is located to the left (west) side of the duplex with the letter "A" located above the front door. Unit "A" faces south. The duplex premises is surrounded by a fence with brown wooden posts and top railing. The warrant also extends to all buildings, structures, vehicles, and appurtenances on the curtilage of that part of the duplex premises associated with Unit A, including any vehicles parked inside and in front of the garage associated with Unit A. The following are recent photographs of the premises:





ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8); any visual depiction of a minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8), or to the possession, receipt, or distribution of a visual depiction of a minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and to the identification of individuals involved in such activities.

3. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

4. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider and any Telecommunications Service Provider.

5. Any and all visual depictions of minors.

6. Any and all diaries, notebooks, notes, and any other records, including address books, names, and lists of names and addresses, pertaining to minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section

2256(2); or reflecting personal contact and any other activities with such minors.

7. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, of any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact, or any other activities with, minors.

11. Any and all computer hardware, meaning any and all computer equipment. Computer hardware includes all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or

data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanner, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

12. Any and all computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software includes data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

13. Any and all items which are used, or could be used, to store digital data, including, but not limited to, zip disks, floppy diskettes, compact disks, DVDs, music players, USB storage devices, Firewire storage devices, computer hard disk drives, optical storage devices, and flash memory devices.

14. Any and all computer-related documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

15. Data security devices, meaning any devices, programs, or data - whether themselves in the nature of hardware or software - that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software,

computer-related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

16. Any and all mobile communication devices (hereinafter referred to as the "Subject Devices") and all accessories, devices, and other things associated with the Subject Devices, including, but not limited to:

a. Any and all mobile storage devices intended to be used with the Subject Devices, including memory cards, memory sticks or other media upon which data can be stored.

b. Any and all power cables, software, instruction books, connection cables, synchronization cables, or any other connection devices used to provide power, connectivity to another device or computer, synchronization, computer usage, or instructions for use of the Subject Devices.

c. Any and all other accessories associated with the Subject Devices, or in such proximity to the Subject Device (including on the person from whom the Subject Devices may be seized) as to infer their pending, continual, or intended usage with the Subject Devices.

d. Any and all items, cards, devices, and other things which are connected to or inserted into the Subject Devices at time it is seized.

e. Any and all documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the Subject Devices, software, or any accessories.

f. Any and all data security devices, meaning any devices, programs, or data - whether themselves in the nature of hardware or software - that can be used or are designed to

be used to restrict access to, or to facilitate concealment of, the Subject Devices, or any associated computer hardware, computer software, computer-related documentation, or electronic data. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

17. Any and all photographic and other image-producing devices, including, but not limited to, digital cameras, film cameras, Polaroid cameras, video cameras, web-cameras, and other devices used to produce an image or visual depiction of another individual; and any film, videotape, or other medium used to produce or store visual images.

18. Any document, record, or item that may be evidence of the location of any occupant of 414A W. Dittmar Road, Austin, Texas 78745, for the period February 1, 2015, to the present.

19. Any document, item, or record that may bear a relationship to the username "marleyboy."

20. Any document, item, or record pertaining to "Website A" or any member or user of "Website A," including any correspondence, e-mails, electronic messages, and records pertaining to "Website A," or the identity of any member/user of "Website A."

21. All documents and records evidencing ownership or any other interest in: any residence, dwelling, business, or storage location; and any of the aforementioned items, internet service accounts or locations.

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Western District of TexasIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)414A W. Dittmar Road, Austin, Texas 78745,
and all buildings, structures, vehicles, and
appurtenances on the curtilage thereof

Case No.

1:15-M-627

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of Texas

(identify the person or describe the property to be searched and give its location):

414A W. Dittmar Road, Austin, Texas 78745, and all buildings, structures, vehicles, and appurtenances on the
curtilage thereof, which is more specifically described in Attachment A.The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before

12-28-2015

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

12-14-2015 125 p.m.

City and state: Austin, Texas

Judge's signature

Mark Lane

United States Magistrate Judge

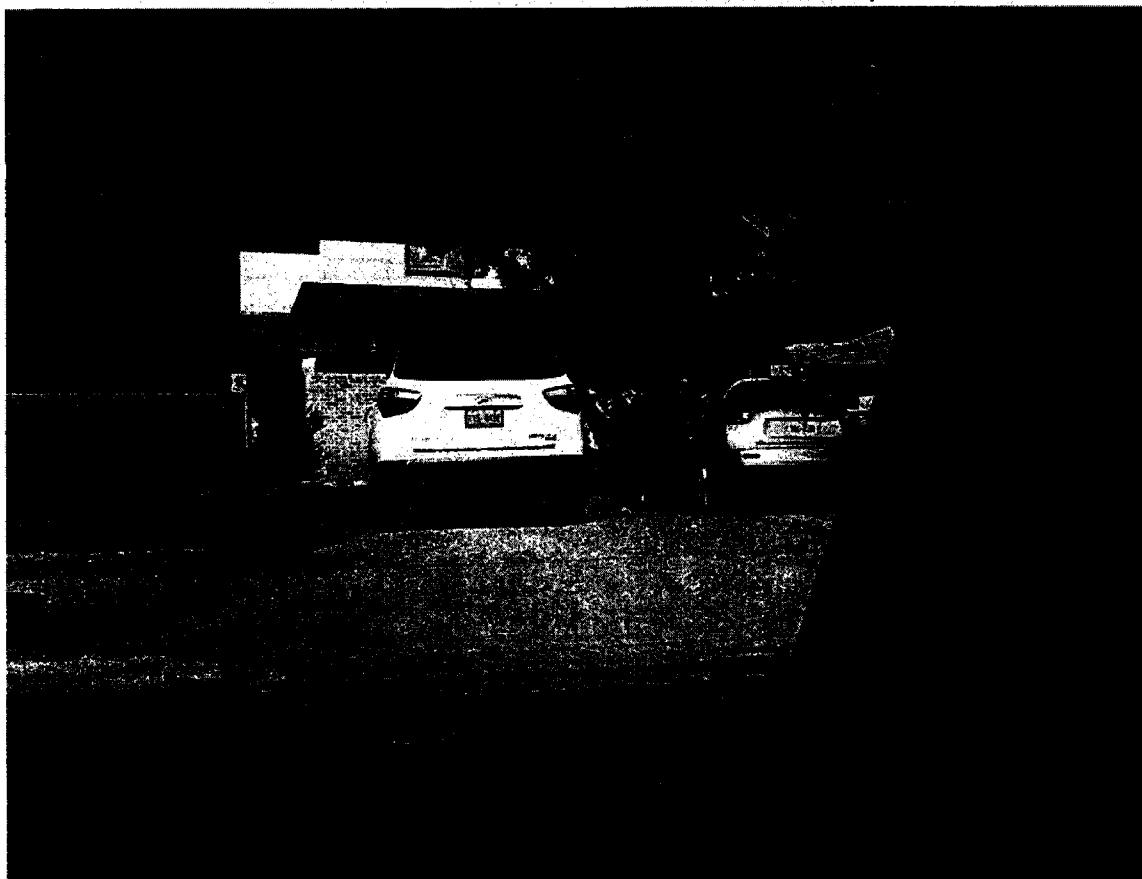
Printed name and title

[illegible]

ATTACHMENT A**DESCRIPTION OF PROPERTY TO BE SEARCHED**

The premises known as at 414A W. Dittmar Road, Austin, Texas 78745, also referred to as Unit A of 414 W. Dittmar Road, is more particularly described as two-family, two-story duplex comprised of tan and brown brick on the lower level with tan hardie-siding on the upper level. The duplex faces south and has a driveway leading from the street (West Dittmar Road) to the two garage doors located in the middle. The front doors are located on the far left (west) and far right (east) of the duplex with a sidewalk leading up to each door from the driveway. Unit "A" is located to the left (west) side of the duplex with the letter "A" located above the front door. Unit "A" faces south. The duplex premises is surrounded by a fence with brown wooden posts and top railing. The warrant also extends to all buildings, structures, vehicles, and appurtenances on the curtilage of that part of the duplex premises associated with Unit A, including any vehicles parked inside and in front of the garage associated with Unit A. The following are recent photographs of the premises:





ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8); any visual depiction of a minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8), or to the possession, receipt, or distribution of a visual depiction of a minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and to the identification of individuals involved in such activities.

3. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

4. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider and any Telecommunications Service Provider.

5. Any and all visual depictions of minors.

6. Any and all diaries, notebooks, notes, and any other records, including address books, names, and lists of names and addresses, pertaining to minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section

2256(2); or reflecting personal contact and any other activities with such minors.

7. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, of any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact, or any other activities with, minors.

11. Any and all computer hardware, meaning any and all computer equipment. Computer hardware includes all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or

data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanner, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

12. Any and all computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software includes data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

13. Any and all items which are used, or could be used, to store digital data, including, but not limited to, zip disks, floppy diskettes, compact disks, DVDs, music players, USB storage devices, Firewire storage devices, computer hard disk drives, optical storage devices, and flash memory devices.

14. Any and all computer-related documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

15. Data security devices, meaning any devices, programs, or data - whether themselves in the nature of hardware or software - that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software,

computer-related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

16. Any and all mobile communication devices (hereinafter referred to as the "Subject Devices") and all accessories, devices, and other things associated with the Subject Devices, including, but not limited to:

a. Any and all mobile storage devices intended to be used with the Subject Devices, including memory cards, memory sticks or other media upon which data can be stored.

b. Any and all power cables, software, instruction books, connection cables, synchronization cables, or any other connection devices used to provide power, connectivity to another device or computer, synchronization, computer usage, or instructions for use of the Subject Devices.

c. Any and all other accessories associated with the Subject Devices, or in such proximity to the Subject Device (including on the person from whom the Subject Devices may be seized) as to infer their pending, continual, or intended usage with the Subject Devices.

d. Any and all items, cards, devices, and other things which are connected to or inserted into the Subject Devices at time it is seized.

e. Any and all documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the Subject Devices, software, or any accessories.

f. Any and all data security devices, meaning any devices, programs, or data - whether themselves in the nature of hardware or software - that can be used or are designed to

be used to restrict access to, or to facilitate concealment of, the Subject Devices, or any associated computer hardware, computer software, computer-related documentation, or electronic data. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

17. Any and all photographic and other image-producing devices, including, but not limited to, digital cameras, film cameras, Polaroid cameras, video cameras, web-cameras, and other devices used to produce an image or visual depiction of another individual; and any film, videotape, or other medium used to produce or store visual images.

18. Any document, record, or item that may be evidence of the location of any occupant of 414A W. Dittmar Road, Austin, Texas 78745, for the period February 1, 2015, to the present.

19. Any document, item, or record that may bear a relationship to the username "marleyboy."

20. Any document, item, or record pertaining to "Website A" or any member or user of "Website A," including any correspondence, e-mails, electronic messages, and records pertaining to "Website A," or the identity of any member/user of "Website A."

21. All documents and records evidencing ownership or any other interest in: any residence, dwelling, business, or storage location; and any of the aforementioned items, internet service accounts or locations.